UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/670,783	09/27/2000	Joseph Andrew Mellmer	1909.2.74A	6748

7590 04/19/2005

James D. Liles
Dinsmore & Shohl LLP
255 East Fifth Street
1900 Chemed Center
Cincinnati, OH 45202

EXAMINER	
WOO, ISAAC M	
ART UNIT	PAPER NUMBER
2162	

DATE MAILED: 04/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## *Office Action Summary*	**Application No.** 09/670,783	**Applicant(s)** MELLMER ET AL.
	Examiner Isaac M Woo	**Art Unit** 2162

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 28 February 2005.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-101* is/are pending in the application.

4a) Of the above claim(s) *59-89* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-58 and 90-101* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

45

DETAILED ACTION

1. This action is in response to Applicant's Amendments, filed on February 28, 2005 have been considered but are deemed moot in view of new ground of rejections below.

2. Claims 1, 25, 58, 90, 98 and 101 are amended. Claims 1-58 and 90-101 are pending.

3. The objection to the claims 29-30 has been withdrawn because of the amendment.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-58 and 90-101 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chang et al (U.S. Patent No. 6,157,953, hereinafter, "Chang") in view of Van Dyke et al (U.S. Patent No. 6,412,070, hereinafter, "Van").

With respect to claim 1, Chang discloses, database (user profile data repository, col. 4, lines 7-27) including a vault for storage of at least one user object (user profile data, col. 4, lines 7-27) for a user, the user object having a corresponding safe object (user identifier, col. 3, lines 13-65, user profile data repository, col. 4, lines 7-27, user identifier is used to security (safe object)), the safe object containing at least one profile accessed and administered exclusively by the user at the exclusion of the system administrator (the user who can grant access right for system administrator, user profile data repository, col. 4, lines 7-27), each profile including digital identity information provided by the user (user identifier, col. 3, lines 13-67, access control mechanism derives a list of services to which the system administrator associated with the identifier and password has administrative access). Chang does not exclusively disclose, having access rights granted to a system administrator, operable to be shared with other users having' other profiles accessible and administered exclusively by the other users, the string occurring exclusively upon initiation by the user. However, Van discloses, "As illustrated in FIG. 7, one type of user 145, Domain Adminstrator, are granted all of these control access right", see (fig. 7, col. 9, lines 47-59). This teaches granting access rights granted to a system administrator. Van discloses, "A user 145 can grant control rights to another user 145 by manually pressing the "Add" button of administrative tool 400 and selecting the control rights from a list of "properties" associated with the user object class. FIG. 10 shows administrative tool 400 displaying control rights along with all the other individual properties of the user object after a user 145 presses the "Add" button", see (col. 10, lines 6-19). User(s) is "Add" means that the users can share with other added users. “Not added users” are administered exclusively by the user who can control access right on fig. 7. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Chang by incorporating having access rights granted to a system administrator, operable to be shared with other users having' other profiles accessible and administered exclusively by the other users, the string occurring exclusively upon initiation by the user. One having ordinary skill in the art at the time the invention was made would have been motivated to use such a combination because that would provide Chang's system the enhanced and extended capability of access control system in multi-user sharing network system environment.

With respect to claim 2, Chang discloses, one safe object contains more than one user-administered profile and different profiles provide sets of different digital identity information about the user, see (col. 4, lines 7-27).

With respect to claim 3, Chang discloses, the safe object also contains at least one user-administered contact, each contact representing an entity outside the user's safe which receives controlled read access to digital identity information from at least one of the profiles, see (col. 6, lines 11-49).

With respect to claim 4, Chang discloses, safe object also contains at least one drop box object, see (col. 6, lines 11-49).

With respect to claim 5, Chang discloses, one application object with settings for an application, see (col. 6, lines 11-49).

With respect to claim 6, Chang discloses, one view object see (col. 6, lines 11-49).

With respect to claim 7, Chang discloses, one access object, see (col. 3, lines 13-65, user identifier for access).

With respect to claims 8, Chang discloses, web server and an identity server, see (col. 3, lines 13-65).

With respect to claims 9, Chang discloses, the identity server communicate using encrypted user names, see (col. 6, lines 11-49).

With respect to claim 10, Chang discloses, web server and the identity server are secured by a firewall, see (col. 3, lines 13-65, user identifier for access with secure).

With respect to claim 11, Chang discloses, identity server appliance, see (108, server, fig. 1, col. 1, lines 55-65).

With respect to claim 12, Chang discloses, a zero-byte client, see (col. 6, lines 11-49).

With respect to claim 13, Chang discloses, installed client, see (104, client, web, user host, fig. 1, col. 1, lines 55-65).

With respect to claim 14, Chang discloses, system comprises a provider model for access to the database, see (col. 1, lines 5-67 to col. 2, lines 1-65).

With respect to claim 15, Chang discloses, abstract model offers a hierarchical storage system in a representation that includes a user, a container, and data, see (212, database, col. 6, lines 10-35).

With respect to claim 16, Chang discloses, programmatic interface to identity items and operations that correspond generally to directory service objects, see (col. 1, lines 5-67 to col. 2, lines 1-65).

With respect to claim 17, Chang discloses, wherein the database includes multiple safe objects contained in a vault object, see (col. 2, lines 1-65).

With respect to claim 18, Chang discloses, each vault object contains at least one user safe object, and objects contained by the safe objects are federated to provide controlled access between the vault servers, see (col. 1, lines 5-67, user identifier).

With respect to claim 19, Chang discloses, Universal Resource Identifier which specifies at least a protocol, a host, a path, and an object, see (web based network system, col. 12, lines 1-19).

With respect to claim 20, Chang discloses, digital business card application object having a corresponding profile object which includes digital identity information provided by the user, see (col. 2, lines 1-65).

With respect to claim 21, Chang discloses, system comprises a means for one user to receive updated profile information of another user using a link to the database partitioned directory services database, see (col. 5, lines 38-62).

With respect to claim 22, Chang discloses, partitioned directory services database, see (col. 5, lines 38-62).

With respect to claim 23, Chang discloses, account creation service which creates a new account for a user based on a template, see (col. 2, lines 1-65).

With respect to claim 24, Chang discloses, a safe management service which provides an administrative tool to manage and maintain safe objects, see (col. 5, lines 3-35).

With respect to claim 25, Chang discloses, schema management service which permits an administrator to at least view a directory service schema, see (col. 5, lines 3-35).

With respect to claim 26, Chang discloses, batch account creation service which creates several accounts at one time, see (col. 5, lines 3-35, creating user account by system administrator).

With respect to claim 27, Chang discloses, install service which permits one to install and configure an identity server, see (col. 5, lines 3-35).

With respect to claim 28, Chang discloses backup and restore service which allows one to backup and restore at least one safe object, see (col. 5, lines 3-35).

With respect to claim 29, Chang discloses, safe advisor service which allows one to verify the integrity of a safe object, see (col. 3, lines 13-65).

With respect to claim 30, Chang discloses, legal recovery tool which recovers digital identity information for forensic use, data demoralization service which facilitates data transformation on database fields, see (col. 3, lines 13-65).

With respect to claims 31, Chang discloses, data denormalization service which facilitates data transformation on database fields, see (col. 3, lines 13-65, by database management system).

With respect to claim 32, Chang discloses, rules service, see (col. 3, lines 15-67 to col. 4, lines 1-25).

With respect to claim 33, Chang discloses, identity server to register interest in and be notified of changes in the database, see (col. 4, lines 1-25).

With respect to claim 34, Chang discloses, event service which allows an identity server to register interest in and be notified of changes in the database, see (col. 5, lines 3-37).

With respect to claim 35, Chang discloses, process to verify information gathered from a user registration form, see (col. 6, lines 1-35, user ID is used for verification).

With respect to claim 36, Chang discloses, profile discovery and publishing service which allows users to publish at least a portion of their profile information, see (col. 6, lines 1-35).

With respect to claim 37, Chang discloses, allows a user to have the service fill in at least part of an online form with information from one of the user's profile objects, see (fig. 3, col. 7, lines 35-65).

With respect to claim 38, Chang discloses, form conversion service which assists a webmaster in converting existing forming to standardized field names, see (col. 7, lines 35-65).

With respect to claim 39, Chang discloses, install service which installs servlets on a web server, see (col. 1, lines 3-37).

With respect to claim 40, Chang discloses, identity exchange service for portions of a privacy protection protocol, see (col. 6, lines 11-36).

With respect to claim 41, Chang discloses, chat service which sets up chat rooms so users can communicate with each other in real time, see (col. 3, lines 15-67 to col. 4, lines 1-25).

With respect to claim 42, Chang discloses, presence service which lets users specify where they are and allows them to discover another user's presence information, see (fig. 2, col. 6, lines 37-67).

With respect to claim 43, Chang discloses, anonymous remailer service which allows users to choose different email addresses for different profiles, see (fig. 2, col. 6, lines 37-67).

With respect to claim 44, Chang discloses, anonymous browsing service which allows a user to browse a network in an anonymous fashion to prevent sites from collecting user identity information, see (fig. 2, col. 6, lines 37-67).

With respect to claim 45, Chang discloses, infomediary service which facilitates creating an infomediary, see (fig. 2, col. 6, lines 37-67).

With respect to claim 46, Chang discloses, tracking IP addresses in order to selectively publish the last known IP address of a user, see (col. 9, lines 11-43).

With respect to claim 47, Chang discloses, underlying directory service and an underlying file system in order to enforce access controls on web pages published by users, see (col. 9, lines 11-43).

With respect to claim 48, Chang discloses, email services, encodes contact relationship information in the user's email address, see (col. 9, lines 11-43).

With respect to claim 49, Chang discloses, contact relationship information in the user's email address, see (col. 9, lines 11-43).

With respect to claim 50, Chang discloses, profiles to filter email sent to the user, see (col. 9, lines 11-43).

With respect to claim 51, Chang discloses, determining whether a user logging in at a third party web site is registered as a user of the system, see (col. 7, lines 20-34).

With respect to claim 52, Chang discloses, logging the user into the system if the user is registered, and a means for registering the user and logging the user in if the user was not registered, see (col. 7, lines 20-34).

With respect to claim 53, Chang discloses, registering the user and logging the user in comprises a means for capturing user login information for the third party web site, see (col. 7, lines 20-34).

With respect to claim 54, Chang discloses, user digital identity information is only made available to a partner site if the user has flagged the information as public, see (col. 7, lines 35-64).

With respect to claim 55, Chang discloses, icon provides a transaction history, see (col. 7, lines 35-64).

With respect to claim 56, Chang discloses, user authentication mechanism, see (col. 7, lines 35-64).

With respect to claim 57, Chang discloses, launch point for launching application, see (col. 5, lines 38-62).

With respect to claim 58, Chang discloses, non-repudiation feature whereby an administrator cannot change a user password and then log on as the user, see (col. 12, lines 32-44).

With respect to claims 90 and 98, Chang discloses, vault for storage (user profile data repository, col. 4, lines 7-27) of one or more safes of digital identities (user profile, Information relating to each user is stored in database 212 and information entered by a user is authenticated against this information. The information, or credentials, if verified, is passed through a CGI program to the service hosts indicated by the user. Once received by the service hosts the information is re-authenticated against the user profile in the database on behalf of the system administrator; in other words, this is done "behind the scenes" without intervention or any extra steps from the user. The user only has to log on (i.e. enter certain information such as name and password) to the management console through a browser once and this information is passed on to the service hosts automatically), see (col. 12, lines 32-43), the vault including an access protocol layer (col. 6, lines 1-36), an identity server layer (col. 6, lines 1-36, access control for servers), and an identity manager layer (fig. 7, administrator right for user, col. 6, lines 37-67 to col. 7, lines 1-34). Chang does not exclusively disclose, having access rights granted to one or more system administrators including management of one or more accounts of end users, the one or more safes of digital identities having access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators. However, Van discloses, “As illustrated in FIG. 7, one type of user 145, Domain Adminstrator, are granted all of these control access right”, see (fig. 7, col. 9, lines 47-59). This teaches granting access rights granted to a system administrator. Van discloses, “A user 145 can grant control rights to another user 145 by manually pressing the "Add" button of administrative tool 400 and selecting the control rights from a list of "properties" associated with the user object class. FIG. 10 shows administrative tool 400 displaying control rights along with all the other individual properties of the user object after a user 145 presses the "Add" button”, see (col. 10, lines 6-19). User(s) “Add” means that the users can share with other added users. “Not added users” are administered exclusively by the user who can control access right on fig. 7. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention was made to modify Chang by incorporating having access rights granted to one or more system administrators including management of one or more accounts of end users, the one or more safes of digital identities having access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators. One having ordinary skill in the art at the time the invention was made would have been motivated to use such a combination because that would provide Chang's system the enhanced and extended capability of access control system in multi-user sharing network system environment

With respect to claim 91, Chang discloses, access protocol layer includes one or more protocols selected from LDAP, XML, RPC-over-HTTP, XDAP or SMTP, see (col. 6, lines 11-49).

With respect to claim 92, Chang discloses, server layer serves as an NDS access point, see (col. 7, lines 20-34).

With respect to claim 93, Chang discloses, server layer maintains access rights to the digital identities, see (col. 7, lines 20-34).

With respect to claim 94, Chang discloses, manager layer includes NDS authentication, see (col. 5, lines 13-67).

With respect to claim 95, Chang discloses, identity manager layer has a secret store, including servlets and applets, comprising a vault for secure storage of one or more safes of digital identity profiles, see (col. 6, lines 11-49).

With respect to claim 96, Chang discloses, an identity server, apportioned between a client, a web server and an identity server, see (col. 6, lines 11-49).

With respect to claim 97, Chang discloses, vault for secure storage of one or more safes of digital identity profiles, see (col. 6, lines 11-49).

With respect to claim 99, Chang discloses, identity manager layer, zero-byte client interface, see (col. 6, lines 1-65).

With respect to claim 100, Chang discloses, client application interface user object and a corresponding safe object, the safe object containing at least one profile of the digital identity profiles administered by a user, see (col. 7, lines 4-67).

With respect to claim 101, Chang discloses, user object and a corresponding safe object, the safe object containing at least one profile of the digital identity profiles administered by a user, see (col. 8, lines 1-67).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Isaac M Woo whose telephone number is (571) 272-4043. The examiner can normally be reached on 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E Breene can be reached on (571) 272-4107. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

IMW
April 15, 2005

JEAN M. CORRIELUS
PRIMARY EXAMINER